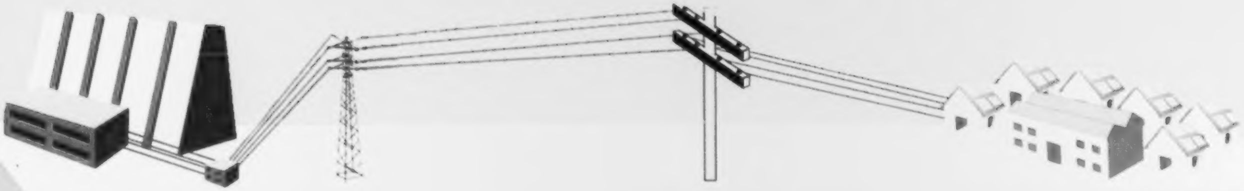
Operationalizing *Privacy by Design*: The Ontario Smart Grid Case Study



Information & Privacy Commissioner,
Ontario, Canada

An initiative supported by:

February 2011

Acknowledgements

I would like to gratefully acknowledge the contributions of the entire *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study* project Steering Committee and Working Group.

Steering Committee Members are: Ken Anderson, Assistant Commissioner (Privacy), IPC; Michael Winters, Chief Information Officer, Hydro One; Rick Stevens, Vice President Asset Management, Hydro One; Steven Ferencie, Partner, Strategy & Transformation, Global Business Services, IBM; Nuala O'Connor Kelly, Senior Counsel for Information Governance and Senior Privacy Leader, GE; and Jeff Meyers, Smart Grid Leader, Telvent.

Working Group Members are: Michelle Chibba, Director of Policy, IPC; Catherine Thompson, Regulatory and Policy Advisor, IPC; Jim Hall, Manager Business Development and Support, Hydro One (Project Chair), Nargis Ladha, Manager Geospatial Systems & Technology Projects, Hydro One; Peter Ruppert, Solution Architect, Advanced Distribution Solution (ADS) Program, IBM; Steven Dougherty, Security and Privacy Specialist, ADS Program, IBM; Ryan Vinelli, Office of the Senior Counsel, Information Governance and Privacy, GE; Byron Flynn, GE; Scott Koehler, Director, Smart Grid Product Management, Telvent.

Information and Privacy Commissioner,
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Foreword

In order to operationalize privacy, it must play a central role — placed at the heart of innovation. To do so organizations must make privacy an essential design feature that figures prominently in the very architecture of the system being contemplated.

I have heard from some utilities that implementation of the Smart Grid is so large and complex that introducing privacy at this point in its development is far too complicated. This paper illustrates that it is in fact simpler and less expensive to incorporate privacy, right from the outset!

The concept of *Privacy by Design* was developed to address the growing and systemic effects of information technology and large-scale networked infrastructure. It refers to the concept and methodology of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle. I have advanced *Privacy by Design* since the 1990s, and recently developed The 7 *Foundational Principles* which set out how to proactively make privacy the default mode of operation, while maintaining full functionality — a positive-sum, not zero-sum, approach to privacy protection.

In the last year, one of my goals has been to place *Privacy by Design* on the Smart Grid map, first by publishing a white paper with the Future of Privacy Forum entitled, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* released in November 2009. I then wrote a second paper, *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid* with Hydro One Inc. and Toronto Hydro Electric Systems Ltd. in June 2010.

As a member of the GridWise Alliance and the National Institute of Standards and Technology's (NIST) Smart Grid Privacy Working Group, I have proposed the adoption of *Privacy by Design* in relation to the U.S. Smart Grid, with which our electrical system here in Ontario is intertwined. To my great pleasure, *Privacy by Design* has gained wide recognition in these circles, with *Privacy by Design* being recommended as a methodology in NIST's report on Privacy and the Smart Grid (NISTIR 7628, vol. 2).

While improvements to the electrical grid are necessary for the long-term reliability of electricity and environmental sustainability, unless *Privacy by Design* principles are incorporated at the outset, and by default, Smart Grid systems run the risk of unnecessarily collecting and disseminating large amounts of personally identifiable information. I would like to extend my sincere thanks and appreciation for the great collaborative effort between Hydro One, IBM, General Electric and Telvent in taking on the challenge of demonstrating how *Privacy by Design* can and is being operationalized into a major Smart Grid project in Ontario, Canada, and as a result, showing that privacy *and* an improved electrical grid can indeed be achieved in unison, in a positive-sum manner.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

Table of Contents

Introduction

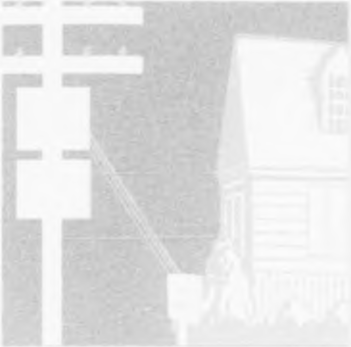
The rate of change in the electrical industry today continues to accelerate, as does the complexity of that change. With the evolution of the Smart Grid, Hydro One and local distribution companies are undertaking large and complex initiatives that will transform our technologies, processes and organization. Because the Smart Grid will potentially encompass the entire utility infrastructure, it is critical to ensure that the proposed solution meets not only electricity infrastructure needs, but also customers' needs.

This paper builds on the Information and Privacy Commissioner of Ontario's previous work with Hydro One in our joint publication *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*, which provides an overview of the Smart Grid in Ontario, the concept of personal information, defines a set of Best Practices for Smart Grid *Privacy by Design*, and provides two use case scenarios. In the present paper, we will directly follow up on the earlier one by answering the question: How can Best Practices for Smart Grid *Privacy by Design* be "operationalized" into Smart Grid systems? The answer is to incorporate these Best Practices into each of the following areas: Smart Grid requirements, business process analysis, architectural decisions, and design considerations, at each step in the development. Such a process will result in the subsequent implementation of Smart Grid solutions that have privacy deeply embedded within them.

Hydro One is currently applying this methodology in relation to a major advanced distribution solution project for its Smart Grid, beginning with a stage known as the "Living Lab" deployment. The Living Lab is an initial deployment that is being used to confirm solution and process details and is made up of a defined subset of its service area in Southern Ontario.

Hydro One shares in this paper how it and its vendor partners, IBM, General Electric ('GE') and Telvent USA Corporation ('Telvent'), are currently laying the privacy groundwork for Hydro One's Smart Grid solutions. With the guidance of the Information and Privacy Commissioner of Ontario, Canada, and the on-the-ground experience of Hydro One, IBM, GE and Telvent, this paper is the first of its kind to demonstrate how to incorporate *Privacy by Design* considerations in developing Smart Grid solutions. It is our hope that this effort will minimize or eliminate any impact on energy consumer privacy for years to come. The paper will demonstrate that by carefully understanding business requirements and processes, operationalizing *Privacy by Design* will lead to choices in architecture and design that will significantly reduce privacy risks, such as the unauthorized dissemination of personally identifiable information, thereby eliminating or diminishing potential impacts on privacy.

This paper is being shared with utilities, vendors and service providers to provide an example of how they can utilize the Best Practices for Smart Grid *Privacy by Design* in the implementation of Smart Grid systems, product design, and energy information services and processes. Policy-makers in the energy field should use this paper as an example of implementing privacy in a pragmatic way — meaning, in a manner where privacy does not lose out to other policy objectives such as energy conservation, but coexists equally with them in a positive-sum manner.



The Hydro One Smart Grid Solution in Ontario, Canada

Hydro One established a long-term vision in 2005 to increase innovation and continue its leading role in providing safe, reliable and cost-effective transmission and distribution of electricity from various supply sources to Ontario electricity users. Hydro One believes that transmission and distribution companies must transform themselves, changing how they do business. Hydro One is focused on innovating and establishing an electricity grid that is modern, flexible and smart — one that will not only support and drive consumer choices about electricity, but set Hydro One on the path to becoming the leading electricity delivery company in North America.

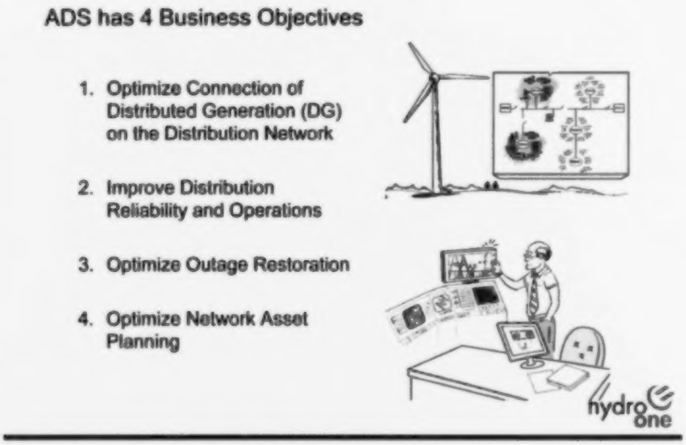
The backbone of the Hydro One vision includes building the means to renew Ontario's power grid. Hydro One plans to do this by innovating and applying new technologies prudently, by driving efficiencies and improvements while balancing service and cost, and by being as productive as possible in the drive to integrate and maximize renewable energy in Ontario. In the first wave of this planned activity, a number of major system improvements were undertaken to enhance the performance of existing infrastructure, relieve internal congestion points, and deliver clean and renewable energy generation. Among these innovations was the introduction of an advanced metering infrastructure; over one million smart meters are now deployed across Hydro One's rural and suburban service area. In concert with the provincial direction on Green Energy and the Smart Grid, Hydro One has begun preparations for the next wave — the Advanced Distribution System (ADS). A key facet of the advanced metering project was the design and implementation of the communications infrastructure — based on the vision established in 2005, Hydro One has been working towards a common communications infrastructure that will also support all the functionality envisioned for the Advanced Distribution System. The underpinning of this communications vision is anchored upon Industry Canada's global leadership by having established nationally licensed spectrum of 30 MHz in the 1800-1830 MHz range for the "Operation, Maintenance and Management of the Electric Supply."[1] Hydro One is using these 30 MHz to deploy a WiMAX network to support its Smart Grid applications.

Hydro One operations require the modeling and control of an increasingly complex electrical transmission and distribution system. A smarter grid will have several different characteristics when compared to today's distribution network. The current electrical distribution system is essentially a one-way instrument, with power flowing from centralized generation sources out through the network to each "load point," meaning to each consumer. The existing system does not rely on any communication from load points, and very little measurement data from anywhere else in the system, to monitor and control the network.

In contrast, the Smart Grid will include a communications network that connects endpoints from consumers, and a number of other sensing and control devices, to make the system more self-aware and controllable. The Smart Grid will also include *distributed generation*, sources of electrical energy located throughout the distribution network. Distributed generation will be primarily in the form of renewable energy such as wind, solar, and biomass. These advances, along with all the other characteristics of the Smart Grid, have the potential to bring significant benefits to Hydro One and its customers. However, implementing these improvements also implies significant changes in the operation of Hydro One's electrical system. Among the most important of these is the need to improve the analysis, automation, and remote control of the distribution grid.

[1] Department of Industry, Radiocommunication Act, Notice No. SMSE-010-09 – New issue of SRSP-301.7, July 11, 2009, Canada Gazette Notice.

The system that is used to automate and control an electrical distribution grid includes a central software component that is called a distribution management system. This software system is a powerful network planning, analysis and operations tool that uses a detailed model of the grid, telemetry and information about power flow patterns to help manage the system in real time. The Advanced Distribution System Project includes the implementation of a distribution management system to meet Hydro One's requirements in Figure 1.



ADS has 4 Business Objectives

1. Optimize Connection of Distributed Generation (DG) on the Distribution Network
2. Improve Distribution Reliability and Operations
3. Optimize Outage Restoration
4. Optimize Network Asset Planning

hydro one

Figure 1 - Business Objectives

With the help of the distribution management system, Hydro One will demonstrate the ability to manage the increasingly complex network of consumer load and distributed resources, along with the existing centralized generation and traditional operating characteristics of the distribution system.

Several core components of Hydro One's Advanced Distribution System program are represented in Figure 2, including the distribution management system which acts as the "brain" of the Hydro One Advanced Distribution System program. A distribution management system is a suite of decision-support software applications which will assist Hydro One's control rooms and field operating personnel in monitoring and controlling the distribution system. Close integration of the distribution management system with other enterprise applications and data stores is essential.

Adding intelligent devices, with automation where appropriate, is another core component of the program and includes an array of devices, equipment, and related software, such as intelligent power equipment (e.g. reclosers, switches, and relays) and monitoring and control devices and subsystems (e.g. power quality monitors, energy storage systems, intelligently controlled capacitor banks to provide voltage support, electronic fault indicators, and dynamic controllers). Hydro One's Advanced Distribution System project also requires a communication network to facilitate communication with intelligent devices. This communication network is used for status and control messages, alerts, etc., to support management of the systems, and operations of the grid.

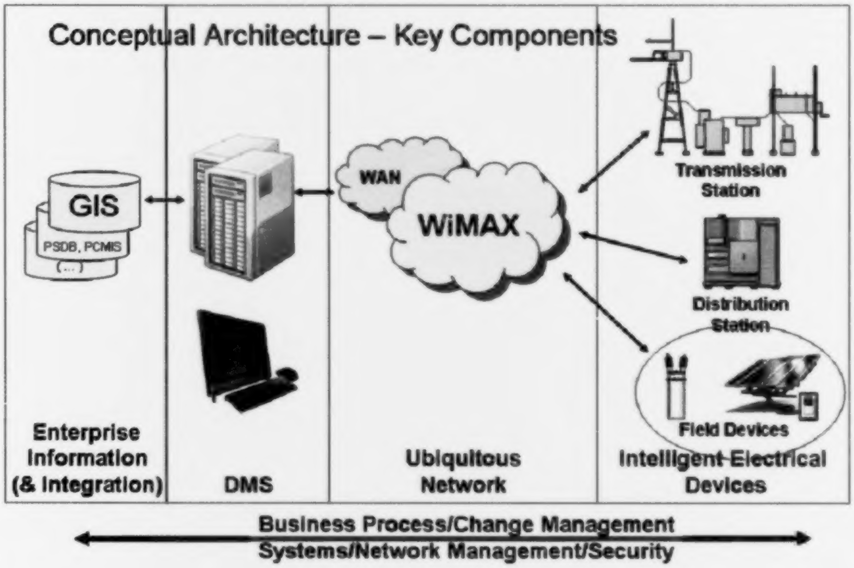

Conceptual Architecture – Key Components
GIS
PSDB, PCMIS
(...)
WAN
WiMAX
Transmission Station
Distribution Station
Field Devices
Enterprise Information (& Integration)
DMS
Ubiquitous Network
Intelligent Electrical Devices
Business Process/Change Management
Systems/Network Management/Security

Figure 2 - Smart Grid Conceptual Architecture

See *Appendix A* for more information on Hydro One's Living Lab.

Operationalizing *Privacy by Design* into Hydro One's Smart Grid

In *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*, the 7 Foundational Principles, originally developed by Ontario Information and Privacy Commissioner Dr. Ann Cavoukian, were adapted to the Smart Grid context. The result was a set of Best Practices for Smart Grid *Privacy by Design*, to aid organizations in understanding foundational privacy concepts that must be incorporated in to the Smart Grid. The Best Practices are as follows:[2]

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring;
2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured;
3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature;
4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects;
5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected;
6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives;
7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement.

Transforming these Best Practices into a concrete reality for Hydro One's Smart Grid partner vendors was a multi-step process. The project began by first defining business objectives (see Figure 1), capabilities and business processes. The adopted methodology had to enable Hydro One to be able to trace privacy requirements from the inception of their business needs, to their fulfilment. In general, this meant including the Best Practices for Smart Grid *Privacy by Design* during the requirements development and design processes, and then following through to subsequently build and test systems for alignment with those requirements, which are detailed in the next section on "Methodology for Operationalization."

Methodology for Operationalization

The successful development of any large-scale networked data system solution that involves or may involve personally identifiable information requires the adoption of a methodology that embeds privacy at the core

[2] See Appendix B for the Best Practices with description.

of the solution's design, starting with an incorporation of *Privacy by Design* into project governance at the earliest stages driving business requirements. The methodology provides a framework that may be tailored to the realities of the operating environment in order to meet the needs of the system, which in this case, is Hydro One's Smart Grid program with its initial deployment in the Living Lab.

Hydro One, working with its lead integrator IBM, employed two methodologies in this project: IBM Intelligent Utility Network and IBM Unified Method Framework. The Intelligent Utility Network framework addresses the convergence in today's utility market of environmental pressures, financial expectations, energy costs, regulatory transparency, aging infrastructure, limited price electricity and improved risk management. This convergence requires a new level of enterprise information and integration to allow for informed decision making.

The Intelligent Utility Network method consists of seven major phases as illustrated in Figure 3 below. Each phase contains a set of activities that may be needed in order to meet the objectives established by Hydro One. The activities and their subsequent deliverables were established in Method Adoption Workshops (MAWS) identifying which of the hundreds of IBM Unified Method Framework deliverables needed to be created in each phase.

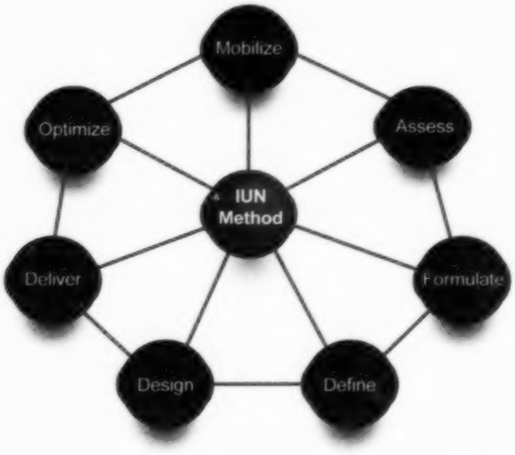


Figure 3 - IUN Phases

The methodology begins with the identification of business requirements, including the Best Practices for Smart Grid *Privacy by Design*, which are incorporated and then traced to the solution deliverables. This traceability then follows the hierarchy defined by Hydro One in their Enterprise Architecture Framework, which defines standards to be applied across various initiatives. This same methodology may be repeated to allow for the coordination of efforts across multiple delivery teams (vendors, project teams, sustaining organization, etc.) and disciplines (IT, power infrastructure, process design, etc.) to contribute to the success of Hydro One's initiatives and overall business objectives.

The Intelligent Utility Network methodology is a phased and iterative process, meaning that in every phase there are inputs and outputs. Some of these are, for example, requirement documents, test results, codes, etc., also referred to collectively as "artefacts" or "deliverables." In the context of the Best Practices for Smart Grid *Privacy by Design*, the first and most important artefact is the Architectural Decisions document. The Architectural Decisions document is a seminal project document that defines policies and principles, and documents the design decisions taken by the project. Specifically, it answers: What are the policies of the organization that will impact the deliverable? What are the design, building, testing and deployment principles that the project will adhere to? What solution deliverable decisions have been adopted, based on the requirements vis-a-vis the policies and principles?

ADS Privacy Risk Assessment

For the ADS Program, a risk assessment was conducted with Hydro One to specifically define the privacy and security requirements for the program. The risk assessment evaluated threat and vulnerability scenarios, the likelihood that the scenario could occur, and the impact of the scenario to Hydro One and its customers. Any applicable privacy requirements were created from the risk assessment and then incorporated into an overall privacy and security architecture.

Operationalizing *Privacy by Design* across Smart Grid Domains

Hydro One uses the concept of "Domains" to classify the possible implications for privacy in the Smart Grid, and to impose certain architectural decisions that will meet privacy requirements, while delivering the necessary functionality. The domains identified are: "Customer Domain," "Services Domain," and "Grid Domain," as illustrated in Figure 4.

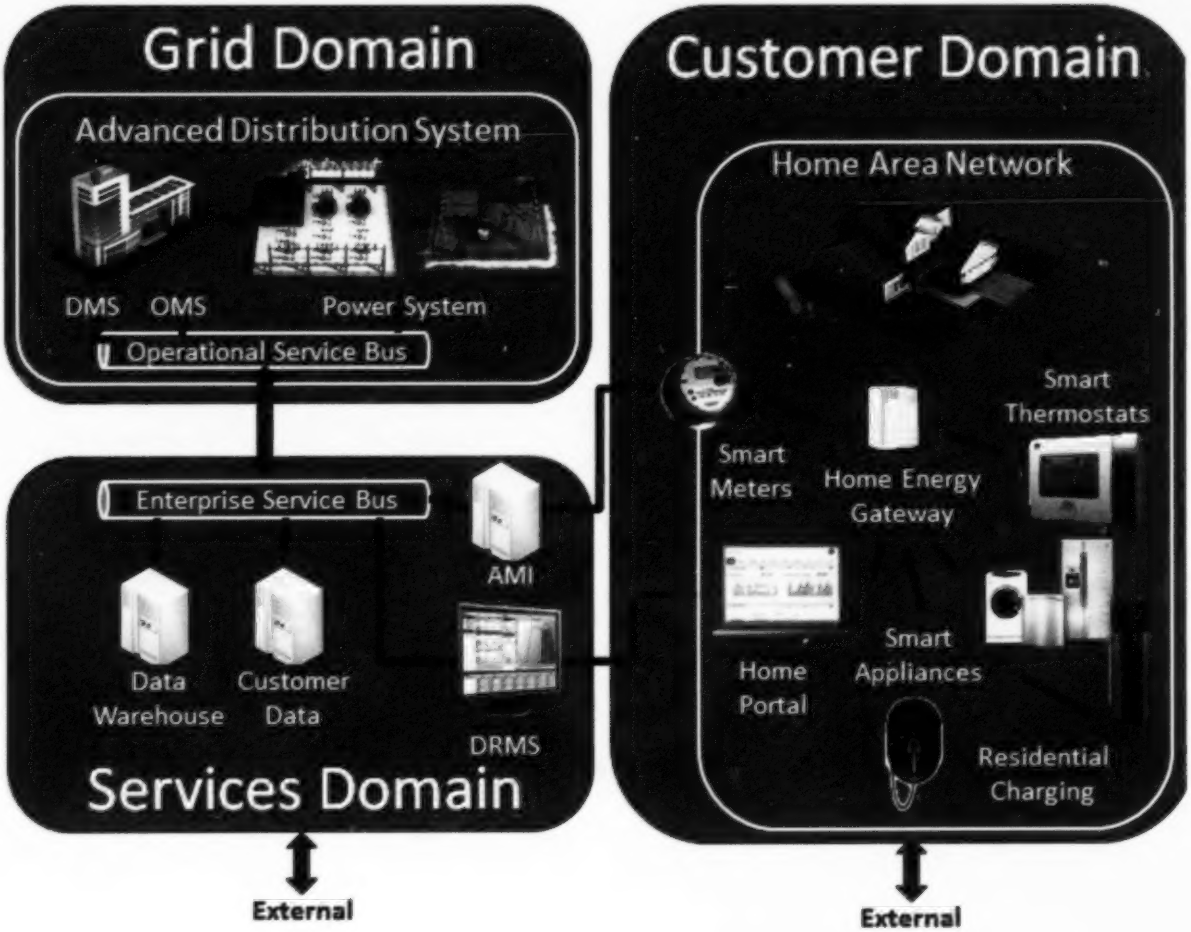


Figure 4 – Grid Domain, Services Domain, and Customer Domain[3]

[3] The acronyms in Figure 4 are as follows: 'DMS' distribution management system, 'OMS' outage management system, 'AMI' advanced metering infrastructure, and 'DRMS' demand response management system.

Customer Domain

The Customer Domain consists of all the devices associated directly with a customer's home. This includes: meters, customer-owned transformers and in-home equipment, be that a Home Area Network or otherwise, such as displays, thermostats, switches, etc. The meter is considered the demarcation point between the customer and Hydro One.

The customer has control over the devices within the home (except for the meter) in terms of what personal information is shared and with whom. If the customer subscribes to any programs or services outside of the power delivery with their utility, the customer would have to grant permission to the utility to operate the devices within the customer's residence. This is an example of the power network evolving from a *passive network* where consumers only use power, receive a bill and settle with their distributor, to a *participatory network* where consumers may also be generators, paying for power at varying rates by time of day, adjusting their consumption by themselves, or subscribing to programs offered by various distributors (or others) to manage their consumption for them. The traditional consumer has now become a participant in the overall management of his or her own energy consumption behavior, as well as a contributor in the management of the grid. In the future, the consumer's management choices will grow considerably thanks to the introduction of products built around Home Area Networks. These products include new smart appliances, displays, energy management applications, home energy gateways, smart electrical vehicle and plug-in hybrid electrical vehicle charging, energy generation and storage.

The participatory network includes functions such as energy demand, power quality and reliability. The Customer Domain involves actions that may influence the quantity or patterns of use of energy consumed by customers, such as actions targeting reduction of peak demand during periods when energy supply systems are constrained. When demand within the power network exceeds supply the system operator must either increase the supply or reduce the demand. Reducing the demand is typically less costly since increasing the supply means engaging more infrastructure such as standby generators or purchasing power in the market. These functions also include the power quality and reliability impacts of new electric and plug-in hybrid electric vehicles and new distributed generation and storage which increase the need for improved demand response management systems by utilities.

As a result, the Smart Grid and metering networks allow for more robust and economical demand management strategies, where information can be collected in real time to identify areas of demand, and properly tailored demand management programs allow for planned reductions in demand. When consumers enrol in such programs, questions inevitably arise such as: How is consumer information protected from the broader network? What limits can consumers place upon possible privacy intrusions and how can consumers withdraw from such programs? How can the devices in homes be connected to the actions within the Grid Domain without compromising privacy?

ADS and the Customer Domain

Specific to the ADS Program, to operationalize the Best Practices for Smart Grid *Privacy by Design* in the Customer Domain, Hydro One included design requirements such as the following as a result of implementing its project methodology:

- No data regarding a customer's identity will persist on any device from the meter to the Hydro One Services Domain — no personally identifiable information will be retained. The customer may choose, however, to purchase additional devices and disclose information to other third parties from their domain (the Customer Domain) which may contain personally identifiable information.

- No information sent to the Customer Domain from the Hydro One Services Domain will include any personally identifiable information that may allow unauthorized recipients to determine the association of the transaction to a specific person or place. All transactions will only include information necessary for the delivery of the information and the information necessary for the transaction to be completed.

For a detailed discussion on Personal Information, please refer to our paper *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid.*

- Any interface provided to the customer for the purposes of program subscription management (e.g. demand management) or power account management will utilize internet (Web) and voice service industry practices for identity management and information protection (e.g. appropriate provisions for the protection of the confidentiality, integrity, and availability of such information).

Services Domain

The Services Domain consists of technology, processes and data used in the delivery of utility services and programs to customers. This includes functions such as billing, power network planning, demand management programs, customer communication programs, etc. The functions within this domain depend upon data and control resources from the Customer and Grid Domains.

For example, meter readings are collected and used within the billing function and may be directly associated to a customer within the Services Domain. This same meter data may also be used for power network planning functions within the Grid Domain, but in a form that is typically not associated directly to a specific customer. Other examples are demand management programs which may request new settings for thermostats, or revenue management which may request the disconnection of service at a meter within predefined parameters. These functions, while associated to a customer in the Services Domain, are not closely associated in the Grid Domain.

ADS and the Services Domain

Specific to the ADS Program, to operationalize the Best Practices for Smart Grid *Privacy by Design* in the Services Domain, Hydro One included design requirements such as the following as a result of implementing its project methodology:

- Access to any device in the Customer Domain from the Services Domain is restricted through authenticated and authorized services published within the Services Domain. All such access will be recorded.

- Direct access to any device within the Customer Domain must be authorized by the customer or customer's agent ensuring separation of duties. Access for a particular process or action is limited to the authorized action and duration. All direct access requests will be logged.

- All applicable systems will support role-based security. Only authorized Hydro One personnel may have access to systems that use customer information. This access is limited to the roles in which the personnel are authorized. This access is authorized and reviewed by designated managers and is managed by system owners.

- Management of all data storage systems must follow the appropriate industry practices.

- All requests made within this domain for an action within another domain will follow the identified operationalized design requirements in the target domain.

- All requests from other domains to this domain will follow operationalized design requirements from the requesting domain.

- All systems will save and archive information in accordance with agreements made between the customer and Hydro One.

Grid Domain

The Grid Domain consists of all systems, processes and devices used for the management of the power network, to ensure the safe and reliable delivery of energy. From generators to high-voltage transmission lines, through substations to medium-voltage distribution lines, on through individual transformers and low-voltage cables, the grid delivers electrical energy to consumers.

Today's grid is monitored and controlled at a limited number of strategic points. Real time monitoring of electric system status occurs at transmission switching stations and substations, as well as substations feeding medium-voltage lines. A limited number of monitoring and control devices currently exist in the medium and low-voltage areas of the system. As the grid evolves into a smarter delivery system, the devices and systems that monitor the grid will grow, adding many more data gathering points. More sensors and smart switches will be added to the medium-voltage system. Smart meters and other intelligent electronic devices will provide monitoring, and limited control, in the low-voltage system.

Smart Meters, while a very important element of the Smart Grid, actually represent a small fraction of the overall grid. The vast majority of the Smart Grid has to do with the operation of the power network rather than pertaining to individual energy customers. Since such operations do not involve individual consumers, transmitters and distributers do not require any personally identifiable information for the operation of power network systems, and can thus be designed to have minimal privacy impact, if any. Since the monitoring and control of the grid does not require the use of any personally identifiable information under normal operations, privacy concerns remain practically non-existent.

Today, information in the Grid Domain is limited to network devices, their status, and their historical performance (e.g. aggregated load profiles, system conditions, operating peaks, maintenance information, etc.). As a result, the sources of data represent nodes on the network — not specific customers. In the future grid, some consumers may be required to be identifiable, in order to support bidirectional operations. For example, those who contribute distributed generation to the grid may need to be identifiable in order to ensure safe operations. While this is an important distinction, it represents the exception, not the norm, and such identification would be known and agreed to by the customer, as a condition of service.

ADS and the Grid Domain

Specific to the ADS Program, to operationalize the Best Practices for Smart Grid *Privacy by Design* in the Grid Domain, Hydro One included design requirements such as the following as a result of implementing its project methodology:

- No data regarding a customer's identity will persist on any device within the Grid Domain — no personally identifiable data will be retained.
- Information regarding a device within the customer domain will be provided through authorized services within the Hydro One Services Domain.
- Access to a device within the Customer Domain must be performed through an authorized service within the Hydro One Services Domain.

Outcome of Operationalizing *Privacy by Design* into Hydro One's Smart Grid

Separation of Domains

Advanced Distribution System (ADS) is designed to function with integration of the Grid Domain from the Services Domain via the implementation of a Services Oriented Architecture. This design will deliver services using transaction and message management tools known in the industry as an Enterprise Services Bus. In this way, separation via the Services Domain is controlled between the Customer Domain and Grid Domain.

For example, information is collected on a scheduled basis or in real time from meters associated with customers or from operational meters, however information read from the meters is limited to energy consumption, power statistics and the meter identifier. Meter readings are stored in an Operational Data Store, where the information can be aggregated dynamically, or an average representative consumption profile can be created on a regular basis. The Operational Data Store does not associate the energy consumption to customers.

The Customer Domain is also isolated from the Grid and Services Domain to provide consumer control over connections in the Services Domain, or remote customer access of their home energy system or remote connection to trusted third parties including energy service providers. Remote and third party connections are to be managed by the customer, and no customer data is made available by the meter to remote connections or third parties unless approved by the end customer.

Grid to Services Domain Management and Privacy

Grid Domain connections to the Services Domain in the Advanced Distribution System (ADS) consists of the Distribution Management System (DMS) and overall Power System facilitating network automation, protection and control. A risk assessment was conducted to define privacy requirements and the privacy and security architecture for the ADS, which in turn have been factored into the design of the Advanced Distribution System DMS.

The Advanced Distribution System uses aggregated average consumption profiles from a meter data system that is segregated from the commercial and personal information of the consumer. For purposes of analyzing the network, the location of the meter's connection to the grid is important, allowing the system to represent load along the length of a particular circuit aggregating load to transformers, substations and the entire system. However, parameters such as a consumer's name, address, and contact information are not relevant for load analysis in the Distribution Management System.

There are cases, though, where personally identifiable information of the consumer could be required by the Advanced Distribution System. For example, if a consumer has a distributed generation source, contact information may be required as a safety precaution in the event of an emergency. In such cases, appropriately authorized services in the Services Domain would be used to separate the personally identifiable information from the Grid management functions.

The above design approach allows the information that is used by the Distribution Management System to perform network state estimation, load flow analysis, and several other advanced functions, to be carried out without the need for personally identifiable information as described in the Appendix.

Demand Response Management and Privacy

The operationalization of the Best Practices for Smart Grid *Privacy by Design* is fundamental to the interaction between the demand response systems in the Grid and Services Domains and the customer in the Customer Domain. Proper operationalization is even more critical because of the ongoing evolution of various utility programs, technologies, consumer energy management applications and consumer expectations.

The demand response management system will be designed with privacy at its core, while maintaining the ability to handle the following functions: receive demand response events from the Independent System Operator via an external connection; receive demand response events from the distribution management system; determine the appropriate demand response control for selected customers; transmit demand response events to the customer via the advanced metering infrastructure or via other communications method; and storage and retrieval of demand response event data in the data warehouse.

Customer Domain Applications

Customer Domain Applications may limit their interaction to within the customer's home, such as when the customer buys and configures a gateway about which the utility has no visibility or knowledge. In the event that these Customer Domain applications are integrated into the Services Domain of the utility, some of the critical privacy elements on the home portal front include: program enrolment and device provisioning; restricting access to authorized users, third party services and devices; limiting the retention of consumer data; future and upcoming demand response event notification; energy and economic value of customer participation in a program; as well as educating the consumer of the value of participating in other programs.

Electric Load Forecasting

One of the critical parameters in the reliable and efficient operation of the grid is *load*. Electrical load varies for each type of consumer, from industrial to commercial to residential. Load also changes with the season, time of day, weather, and a number of other variables. Predicting the demand on the grid, essentially the aggregate of loads for a location, or feeder, or geographic area, or the system as a whole, is a critical aspect of network planning and operations. Forecasting electrical load based on the characteristics of today's consumers and network operational characteristics is a well-known science. In the new grid, however, with opportunities for consumers to manage, shift, and curtail their loads, and even add generation through a variety of distributed energy resources, forecasting load will be a much greater challenge. At the same time, greater access to information at consumer endpoints through advanced metering infrastructure systems will afford utilities like Hydro One better tools to more accurately forecast load which ultimately benefits customers in the form of more reliable and cost-effective electricity.

Understanding load on the system at any point in time, and being able to predict load in the near term (within a few hours), short term (in one to three days), medium term (during a season), and long-term (growth in one to five years or more), is critical to understanding how the electric grid will perform with optimal efficiency and reliability. Load forecasting affects every aspect of network planning and operations, from reconfiguration to balance phasing, switching to relieve congestion and substation or feeder overloads, restoring service after an outage, and planning for new construction to meet growth.

Determining the load on any element of the electric distribution system starts with an estimation of the daily load profile at any customer location. Consumer energy usage data is the key building block for calculating load. Today, for some consumers, peak load is measured by a special demand meter, usually applied to larger consumers like industrial or commercial loads. For most residential consumers, peak demand is estimated using a mathematical model called a load profile. Using historical data for consumers by specific type, utility engineers develop curves to approximate the changes as they vary throughout a 24-hour period. Therefore, in today's grid, the vast majority of load forecasts rely on some form of estimate.

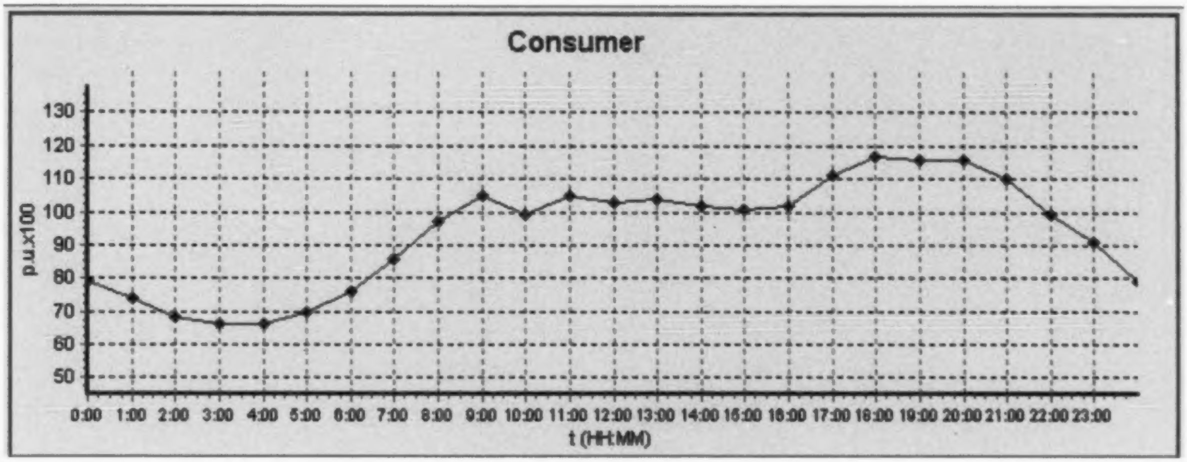
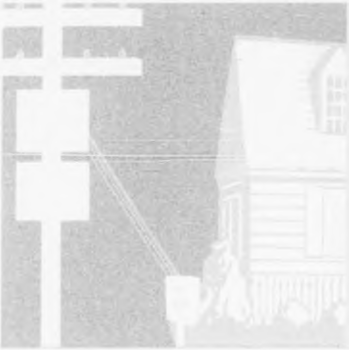


Figure 5 – Example Daily Consumer Load Profile

In the Smart Grid of tomorrow, a customer's daily load profile will not have to be estimated, since it is likely to be measured through the advanced metering infrastructure system. Smart meters will be able to monitor and report peak demand at frequent time intervals, delivering a much more detailed view of how much energy a consumer is using, and when they are using it. As mentioned, this contributes to better load models and management approaches, which ultimately benefit customers in the form of more reliable and cost-effective electricity. In the implementation of the Distribution Management System that Hydro One has designed with its vendors, IBM, GE and Telvent, average hourly customer load profiles will be used to forecast the near term future behaviour of the grid. As these systems become capable of more granular forecasting, the operationalized Best Practices for Smart Grid *Privacy by Design* will guide the development of such advancements.



Conclusion

The grid is comprised of the entire electricity delivery infrastructure. Making it "Smart" is an extremely large and complex endeavour, that is expected to span many years. This, coupled with the fact that many electricity utilities have already started their Smart Grid implementation with the introduction of smart meters, has led some to believe that introducing privacy into the mix, at this early stage, is too complicated a task. This has led them to conclude that they should wait to see how things unfold, and deal with privacy at a later date. No — nothing could be farther from the truth!

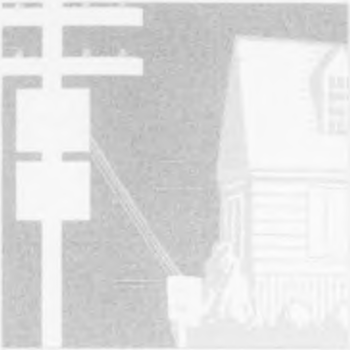
Our first white paper, *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid,* explained why building privacy in from the earliest design stage was ultimately the easiest, fastest, and best way to ensure that privacy considerations would be met. In the present paper, we demonstrate that doing so is not the daunting task that some envision it to be.

Best Practices for Smart Grid *Privacy by Design* will be critical to the successful implementation of a fully utilized Smart Grid. Without the protection of consumer energy use data, lack of consumer confidence and trust will dampen consumer buy-in for the many enabled programs. The Smart Grid is a participatory network where all stakeholders, starting with the consumer, play a very important role in the solution's ultimate success. Energy consumers need to trust that their granular customer energy usage data, made available through the widespread deployment of smart meters and other Smart Grid devices, will be strongly protected.

Over the 100-year history of providing electricity, utilities have striven to attain the highest reputation in the reliability of electricity provision. In the next 100 years, they will also strive to keep up with the increasing pace of change in the industry, while continuing to look out for the customer's best interests, including the privacy of energy consumers' personally identifiable information.

Operationalizing Best Practices for Smart Grid *Privacy by Design* will become increasingly necessary as new smart devices are deployed in the Customer Domain, and as utilities introduce more and more programs.

By assessing the data needs associated with any new applications for the Smart Grid, and by following the 7 Foundational Principles of *Privacy by Design* — engaging in data minimization, and only retaining the data when needed, strong privacy practices will be implemented. By also providing strong protections for confidentiality, integrity and availability, when and where applicable, utilities will be able to achieve the positive-sum goal desired for electricity conservation, reform and good privacy — a true win-win solution that benefits all parties.



Overview of Organizations

Information and Privacy Commissioner, Ontario, Canada

The role of the Information and Privacy Commissioner of Ontario, Canada, is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under the three *Acts*, the Information and Privacy Commissioner: resolves access to information appeals and complaints when government or health-care practitioners and organizations refuse to grant requests for access or correction; investigates complaints with respect to personal information held by government or health-care practitioners and organizations; conducts research into access and privacy issues; comments on proposed government legislation and programs; and educates the public about Ontario's access and privacy laws.

Hydro One Inc.

Hydro One is the largest electricity transmission and distribution company in Ontario. Substantially all of Ontario's electricity transmission system is owned and operated by Hydro One. Its transmission system is one of the largest in North America based on assets, with almost 30,000 km of high-voltage transmission lines. Its distribution system is the largest in Ontario based on assets and spans roughly 75 per cent of the province, with over 123,000 km of wires serving approximately 1.3 million rural and urban customers, local distribution companies connected to the distribution system, and large industrial customers. Hydro One also operates, through its subsidiary, Hydro One Remote Communities Inc., small, regulated generation and distribution systems in a number of remote communities across Northern Ontario that are not connected to Ontario's electricity grid.

IBM Canada

IBM Canada Ltd. is one of Canada's leading providers of advanced information technology, products, services and business consulting expertise. Operating for over 90 years in Canada, IBM is dedicated to helping our clients innovate and realize value through the end-to-end transformation of their business models and the application of smarter technologies and business solutions. IBM Canada is headquartered in Markham, Ontario, and has nationwide responsibilities for sales, marketing and service. IBM's manufacturing and development operations include a semiconductor packaging plant in Bromont, Quebec, and software development laboratory sites in Markham, London and Ottawa, Ontario; Montreal, Quebec; Edmonton, Alberta; and Vancouver and Victoria, British Columbia.

GE Canada

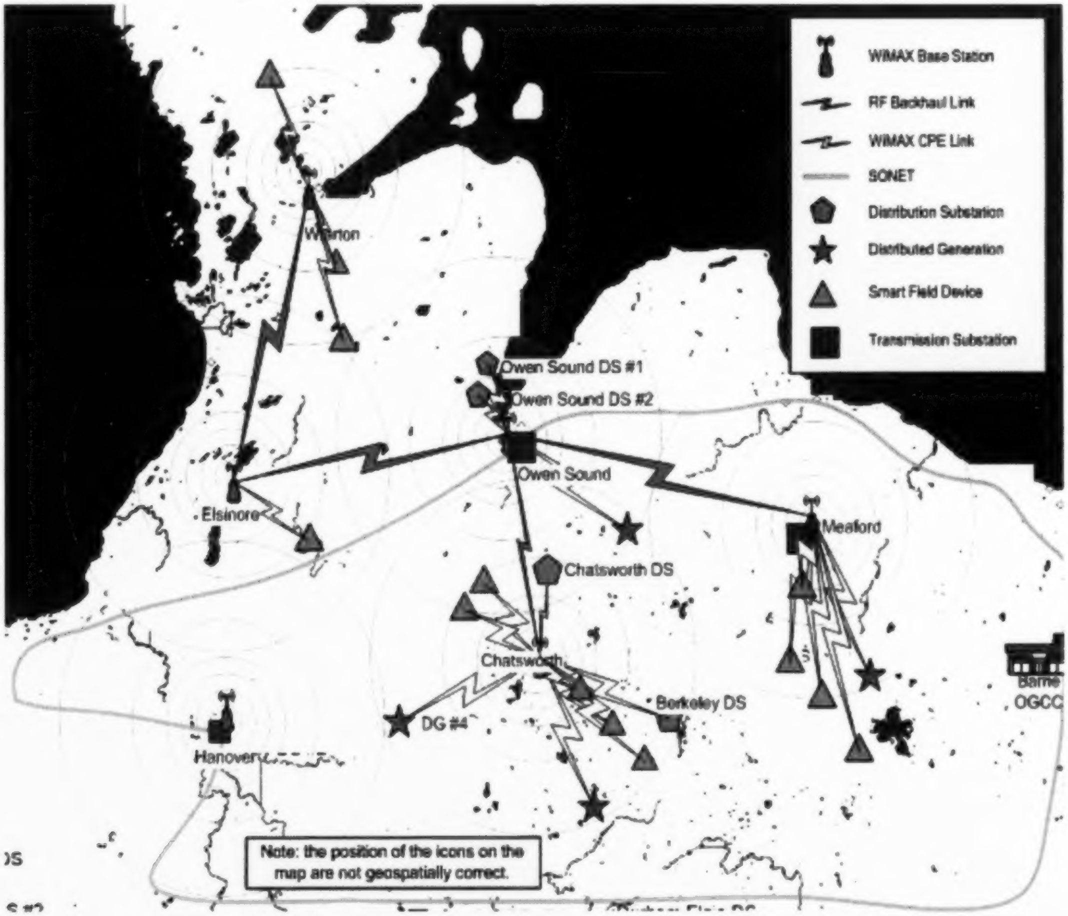
GE is imagination at work. From jet engines to power generation, financial services to water processing, and medical imaging to media content, GE people worldwide are dedicated to turning imaginative ideas into leading products and services that help solve some of the world's toughest problems. GE has operated in Canada for over 100 years, beginning with the manufacturing facility in Peterborough, Ontario, founded by Thomas Edison in 1892. Today, GE Canada has numerous major manufacturing facilities, sales and services locations across the country.

Telvent

Telvent is a global IT solutions and information services provider that improves the efficiency, safety and security of the world's leading companies. Its broad and deep knowledge of infrastructure management systems for utilities puts them in the ideal position to drive the greatest opportunity in today's energy market: the Smart Grid. Utilities everywhere are rapidly planning and deploying networks to transform yesterday's disjointed power distribution grid into tomorrow's Smart Grid, potentially producing enormous gains in energy efficiency, resource conservation and environmental protection. With unparalleled experience in power engineering and grid operations in the electric transmission and distribution networks, Telvent has the insight and expertise needed to turn the promise of the Smart Grid into reality for your utility.

Appendix A – Hydro One Living Lab

Hydro One's first deployment stage of its Smart Grid for advanced distribution will include a subset of its service area in Southern Ontario known as the Living Lab. The figure below is an illustration of part of Hydro One's service area near Owen Sound, Ontario. Those areas offering representative insights for the technology and processes to assist with future rollout will go first in the Living Lab area, followed by other areas in the province in order of priority.



Note: the position of the icons on the map are not geospatially correct.

As may be seen above, several features are being addressed, including substation automation, smart devices and communications network elements.

Appendix B – Best Practices for Smart Grid *Privacy by Design*

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring

Smart Grid projects involving consumer information require privacy considerations to be integrated into their development, right from the project inception phase. Identifying and incorporating privacy considerations into such requirements provides a solid foundation for *Privacy by Design* principles. Project development methodologies are commonly used for the successful development of any large scale networked data system solution (e.g. ISO12207, Unified Process, etc). Include the 7 Foundational Principles of *Privacy by Design* in the requirements development and design processes, and subsequently to the building and testing systems for alignment with those requirements. The utility should conduct Smart Grid project privacy impact assessments (PIA) or similar type of assessments as part of the requirements and design stages, to allow incorporation into requirements and plans — right from the outset. For in-flight projects, the PIA or similar type of assessments can be conducted at a later time in the program if necessary, with any corrective actions incorporated at that time.

2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured

Consumer information, specifically personally identifiable information on the Smart Grid, must be strongly protected, whether at rest or in transit. Personally identifiable information that is communicated wirelessly or over wired networks should be encrypted by default — any exceptions should be assessed (risk-based) on the impact to customers of third party access. It is much harder to protect personal information when it is stored in multiple locations — keep personal information in a minimal number of systems from which it may be securely shared. Similarly, allowing need-only access to this information will provide an extra layer of protection. It is important to consider the manner in which third parties will be allowed to gain access, for various legitimate support purposes — there must be appropriate language built into the contractual agreements to safeguard consumers. There should be as little persistency of personal information as possible. At the end of the cycle, personal information must be securely destroyed, in accordance with any legal requirements.

3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature

Privacy must be a core functionality in the design and architecture of new Smart Grid systems and practices. However, these often involve refreshing the existing asset base, which previously had no real need to carry or transmit consumer information. It is understood that many utilities will be building onto existing legacy systems and that few will be able to work with a clean slate, but instead will need to introduce *Privacy by*

Design principles into legacy systems as opportunities arise, to ensure the overall architecture is secure. It is important to understand how personal information is being handled within the enterprise and determine whether any adjustments need to be made due to challenges raised by new Smart Grid initiatives.

4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects

Beyond making privacy the default by embedding it directly into systems, achieving *Privacy by Design* entails the ability to embed privacy without any loss of functionality of Smart Grid related goals.

5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected

Ensure that the people, processes and technology involved in Smart Grid projects consider privacy at every stage, including at the final point of the secure destruction of personal information.

6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives

Records must be able to show that the methods used to both incorporate privacy as well as the Smart

Grid objectives will meet the privacy requirements of the project. Ensuring such "requirements traceability" between the foundational privacy principles and each stage of Smart Grid project delivery will ensure that one is ready for a third party audit at any time. Any non-compliant privacy deliverables will require an immediate remediation plan to correct the deficiency and provide an acceptable means of redress. Informing consumers of the use to which personal information collected from them will be put is a key objective in achieving visibility and transparency.

7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement

From a consumer perspective, it is essential to provide the necessary information, options, and controls so that consumers may manage their energy, costs, carbon footprints, and privacy.

Appendix C – Advanced Distribution System network state estimation and load flow analysis

In the Grid Domain, there are a number of additional examples for the more advanced practitioner to consider. Examples are included below for the following:

- Feeder optimization and overload management (including a wind illustration);
- Outage management; and
- Power quality management.

Feeder Optimization and Overloading Events

The DMS system has a complete model representation of the electrical network which includes locations where customer load and generation exists.

Feeders represent the wires and devices of the Grid Domain that deliver electricity from stations or substations to consumer loads. When the distributed generation on a feeder exceeds the demand on that same feeder for an interval in time, the direction of power flow may reverse, causing losses and other power quality problems. For this and many other detailed technical reasons, understanding the power flow through continuing changes in load and generation is important to maintaining and improving the reliability of power at any point on the distribution network.

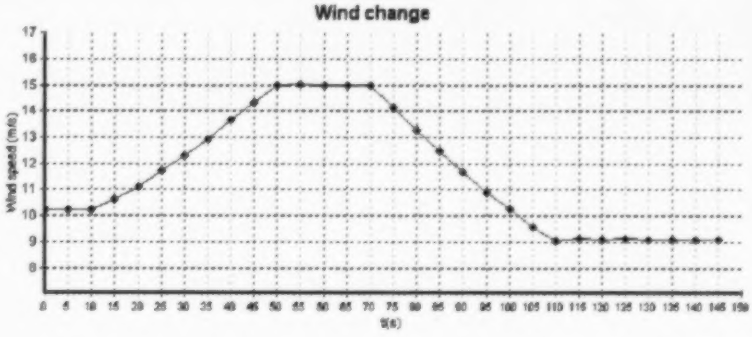


Figure 6 - Wind Effect on Distributed Generation

In a feeder optimization event, aggregate energy load profiles are computed for an area of the distribution system based on advanced metering infrastructure data and real time system measurements. Short-term load forecasting indicates parameters for optimal configuration to support forecasted behaviour of distributed energy resources including distributed

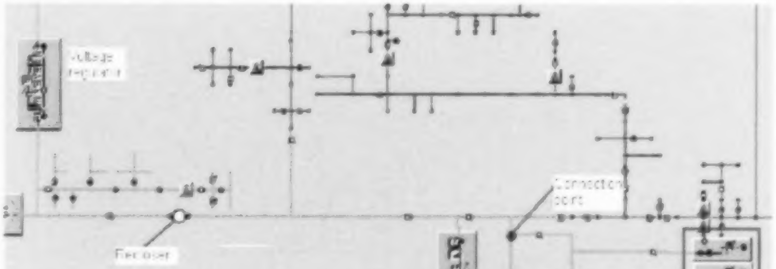


Figure 7 - Feeder Management with Distributed Generation

generation. Renewable sources of energy, such as wind, are a common form of distributed generation, therefore the distribution management system must manage an ever increasingly amount of volatile power sources. The distribution management system executes network switching orders and adjustments to voltage settings, capacitor settings, and relay settings. For example, Figure 6 illustrates how the change in wind speed over the span of several seconds can be quite dramatic. The distribution management system forecasts and monitors changes of this nature to enable optimal performance and reliability for all network locations and for the network as a whole.

In a feeder overloading event, again aggregated energy load profiles are used for the associated area of the distribution system based on advanced metering infrastructure data and real time network measurements. Near-term forecasting indicates the need for customer demand response and load curtailment actions. Demand Response parameters are issued and interruptible load is disconnected as required. The Distribution Management System monitors changes to ensure that optimal performance and reliability is achieved including validation of load curtailment at the required locations on the network. A sample visualization of the various network components involved in managing feeding loading, including distribution generation, is illustrated in Figure 7. This view, combined with zoom and pan functionality to display device statistics in more detail, as well as geographic, i.e. mapping, and single-line diagram views, provide a clear picture to the operator for conducting the operations described above.

Many advanced Distribution Management System functions are leveraged in order to manage these and other network events. All of them require that the system first be provided with representative customer energy load profile data for improved accuracy such as:

- Switch order management;
- Network reconfiguration;
- Voltage regulation;
- Distributed generation management;
- Load forecasting;
- Load reduction and shedding;
- Relay protection;
- Historical analysis; and
- Network planning.

The events described above represent processes that begin with the Grid Domain, and where applications that may involve the Customer Domain are concerned, such as a demand-response request, separation of visibility, authorization and control is achieved through the Services Domain. All of this is accomplished without the Distribution Management System receiving, maintaining, or transmitting any customer personally identifiable information. The Distribution Management System treats meter information the same as any data monitoring: electric power measurements associated with specific locations on the network. And in doing so, personally identifiable information is irrelevant.

Outage Management

Outage data from the smart meters in the Customer Domain is very valuable to the Outage Management System operator. This data is isolated from specific customer information; however, the meter location and outage event on the electrical network is useful for managing the outage. Among other uses, the Outage Management System uses this data to:

- Determine the extent of any outage ;
- Monitor the service restoration after an outage ;
- Update the Voice Response Unit to help inform customers of outage information; and
- Verify outages during 'no light' customer calls.

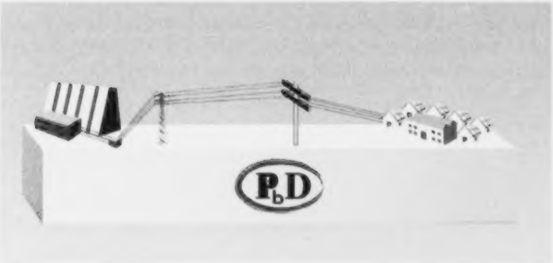
In line with the design principles identified above, visibility to customer information is limited to the events, actions and users with the appropriate level of authenticated access. As outage management systems perform outage location prediction analysis, this is a more detailed analysis unto itself. Nonetheless, the principles of *Privacy by Design* hold true for these areas, as any other.

Power Quality Management

In addition to having power consumption measurements, larger customers, when appropriate, have metering with additional power quality functions. Power Quality data from these smart meters are very valuable to the Advanced Distribution systems including the Distribution Management System assigned to managing the electrical grid. This data is similarly separated from any customer information that is not needed to accomplish the actions required for management of the Grid; of note, the meter location on the electrical network is necessary to manage power quality since it's location on the grid is relevant. Identification of any personal customer information, however, is not required. Among other uses, the Advanced Distribution System uses this data to:

- Improve the voltage profile along the feeder ;
- Reduce distribution losses; and
- Improve load and asset management especially on circuits with significant distributed generation or storage.

Similar to outage management, power quality management is a topic onto itself, and again, the principles of *Privacy by Design* can be held true.



Information and Privacy Commissioner of Ontario, Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

Hydro One Inc.
483 Bay Street
North Tower, 15th Floor Reception
Toronto, Ontario
Canada M5G 2P5
Telephone: 416-345-5000
Website: www.hydroone.com

General Electric Canada
2300 Meadowvale Blvd
Mississauga, Ontario
Canada L5N 5P9

IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
Canada L3R 9Z7

Telvent
4701 Royal Vista Circle
Ft Collins, CO
USA 80528
Website: www.telvent.com/smartgrid

The information contained herein is subject to change without notice. Hydro One Inc, General Electric Canada, IBM Canada Ltd., Telvent and the IPC shall not be liable for technical or editorial errors or omissions contained herein.

February 2011

www.privacybydesign.ca

PbD
www.privacybydesign.ca

Information & Privacy Commissioner,
Ontario, Canada

hydro one

GE

An initiative supported by:

IBM

TELVENT